(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 014 249 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.06.2000 Bulletin 2000/26

(51) Int Cl.[7]: **G06F 1/00**, H04L 29/06

(21) Application number: **99125760.1**

(22) Date of filing: **23.12.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **23.12.1998 US 219854**

(71) Applicant: **Computer Associates Think, Inc.**
Islandia, New York 11749 (US)

(72) Inventor: **White, Clive John**
Workingham, Berkshire (GB)

(74) Representative: **Patentanwälte**
Gesthuysen, von Rohr, Weidener, Häckel
Postfach 10 13 54
45013 Essen (DE)

(54) Method and apparatus for automatic user authentication to a plurality of servers through single logon

(57) A method and apparatus is proposed for providing automatic user access authentication of any user who is a member of a set of authorized users of a computer enterprise from any one of a plurality of geographically dispersed user workstations, onto one of a plurality of predetermined local security servers, through the use of a single log-on. A person server resident on a local security server compares the user-provided identification information to entries contained in a local authentication database. If the person server finds a match, the user is granted access to the local security server. If the person server does not find a match, the person server then searches a network database to determine whether the entered user name is known to the enterprise. If the person server finds a single user name matching the previously entered user name, it returns the name of the local security server associated with the computer enterprise whose local authentication database may have the information necessary for allowing proper authentication of the user. Upon receiving the name of the newly-identified server, the client then automatically retrieves the server's logical location from a service mapping file and then repeats the authentication request to the new local security server.

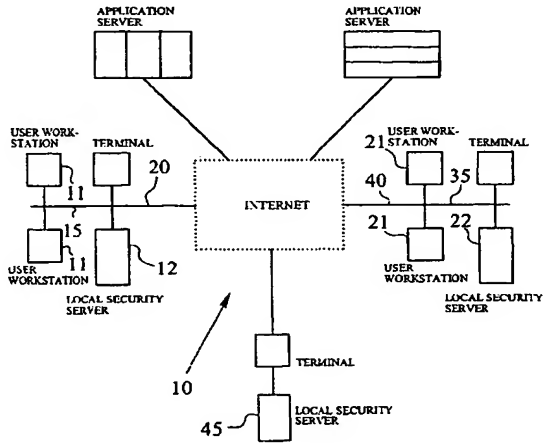

Fig. 1

EP 1 014 249 A1

Description

[0001] This invention relates to an apparatus and method for automating authorized user access to a geographically dispersed network from any one of a plurality of workstations.

[0002] Today's business environment is driven by information, and achieving the most effective use of information technology (IT) is a critical component in any organization's success. But the evolution of IT and its extension into all aspects of corporate and personal life has created increasing challenges - both to IT professionals and end users.

[0003] Over the past decade, the standard model for IT systems has changed significantly. In place of the mainframe-based systems which were controlled from a single, central department, organizations are moving rapidly toward a distributed computing environment where applications and services may reside anywhere on the network on different vendors' hardware and operating systems. The principal reason for connecting computers to networks, and connecting networks to other networks, is to enable computers to work together efficiently, and to simplify sharing of resources.

[0004] Distributed computer systems often have a global extent and may include many thousands of workstations in diverse geographic locations. Such systems are particularly useful to business travelers who may desire to access their network from virtually anywhere in the world. For example, a business traveler at a remote site may want to retrieve the latest cost data, obtain the status of a pending order, place a new order or simply read e-mail. Unfortunately, many client-server networks installed today include a wide variety of independent network server resources that prevent, or at least complicate this task. "Independent" in this context means that the network resource has an independent, as opposed to a shared user database. In an independent network, users who are geographically remote from their home terminals who would like to log onto their home network server are forced to enter routing and authentication information such as a network server ID, user identification and password to access the local independent network resource in which their account is maintained. Forgetting passwords and accessing the wrong service or application are but two of the frustrations that users attempt to eliminate by choosing easily remembered passwords and even writing logon information down in readily accessible places. In doing so, however, they are undermining security. Computer savvy users familiar with network naming conventions can easily overcome the inconvenience of signing onto one's workstation from a remote location while the large majority of other network users must either postpone completing a task or possibly resort to other non-network means of obtaining the information.

[0005] Real and potentially costly risks to modern day computing environments - from malicious or careless employees, hackers, or even espionage are sometimes tolerated to maintain productivity and avoid raising administrative overhead with security measures that hamper legitimate users. Prior art network access services have been developed to address the problems created when users attempt to access distributed networks from remote locations. These services provide user access to remote network resources through the use of authentication data stored in local memory. For example, US - A - 5,483,652 discloses a method and related apparatus for permitting a client entity to request access to a service or resource without knowledge of any more than a common name for the service or resource. Unfortunately, that system characteristically envisions that a user will attempt to access remote network resources (e.g., printers, special computers, and unique files) from his/her workstation and does not provide a capability for the user to either log onto the network or access such resources from remote workstations.

[0006] US - A - 5,598,536, on the other hand, discloses an apparatus and method for providing remote users with access to their local computer network via a remote access network server. In that system, a remote user enters a unique user ID string to gain access to a remote computer. Once the remote user is authenticated, that remote user is granted access to the local network. While this system has overcome many of the inconveniences that existed prior to its conception, it still requires a user to utilize two different authentication strings, depending upon whether he/she is attempting to log onto their local network server from either a local or remotely located workstation.

[0007] US - A - 5,655,077 discloses a method and system for authenticating access to heterogenous computing services from a plurality of user workstations while minimizing the number of user interactions. To gain access to this system a user designates a primary logon provider to provide an initial user interface. The user enters identification information and the computer system executes a logon sequence which first invokes the identified primary logon provider. The system authenticates the collected identification information to provide the user access to the network computer services. If the system logon procedure is not successful, then a logon sequence displays an additional screen to collect additional logon information. The logon sequence then invokes the logon routines of other logon providers to enable them to authenticate already collected identification information without displaying additional user interfaces. While this system attempts to log a user onto a network with the least amount of user interaction, it does require a user to designate a primary logon provider and then enter up to two strings of user authentication information before granting the user access to the network.

[0008] Still another concept for reducing the need for user interaction upon system logon is disclosed in US - A - 5,689,638 which discloses a method and system for

providing access to independent network resources. At system logon, the logon data is stored in the memory of a client computer. When a server is accessed, server authentication data is stored in a cache. System logon data and authorization data can be later applied to access another independent resource without requiring further user interaction. However, this document does not address the problem of authenticating a user from a remote workstation whose default server fails to have stored therein the necessary user information that will allow initial authentication. In other words, if the default server does not recognize the entered user name and password, access to the network is denied.

[0009] An additional problem confronting network users wishing to log onto a remotely located network server is the necessity of communicating across the Internet and interfacing with the multiple protocols that operate on the Internet (e.g., IPX, TCP/IP, NetBEUI, etc.) In the past, a user wishing to communicate across multiple boundaries could not easily do so because of language and communication barriers between the user and the various network entities. The user had to know, and adapt to the specific protocol of each data storage entity in order to communicate requests for information to the entity in cognizable form and to translate information once received. Existing devices are limited in that they simply provide the capability to utilize a single protocol to communicate across the network.

[0010] In the last few years, a number of efforts have been undertaken to develop a standard database protocol, that allows users to communicate across a number of different network protocols. One such standard protocol is the X.500 standard, which was developed by the International Telegraph and Telephone Consultative Committee (CCITT). It provides a standard protocol which reduces the communication barriers presented by the number of different protocols operating on the Internet, and it permits local directories maintained by different entities to communicate with one another. CITT, *The Directory-Overview Concepts, Models, and Services,* X.500 Series Recommendation, Document AP IX-47-E. X.500 allows users to find information such as telephone numbers, addresses and other details of individuals and organizations in a convenient structure. X.500 directories are also characterized by their ability to efficiently handle large volumes of highly distributed information.

[0011] Accordingly, it is an object of the present invention to simplify the task of granting a user access to a heterogenous network by providing an apparatus and method that allows a user to log onto a computer network from any one of a plurality of geographically dispersed user workstations on the network, using the same user name and password, in particular that allows a user to log onto an intranet from any workstation on the enterprise through the use of a single user name, password and user role.

[0012] The above object is achieved by an apparatus according to claim 1 or 8 or a method according to claim 14. Preferred embodiments are subject of the subclaims.

[0013] The subject invention dramatically simplifies the procedures for signing onto a network through the use of a single sign on procedure. Once the user logs on via a logon procedure, such as embodied in the procedure identified as AUTOSECURE™ Single Sign On (SSO) described in the Features Guide for V5.1 entitled "Autosecure SSO," copyrighted by Platinum technology, inc., 1997, wherein a user enters a user name and password, the system does the rest by enabling transparent access to all authorized applications and services and providing a simple, integrated view of the computer network. The single sign on capability functions whether a service is resident on a local or a remote network server, and it lets users sign on anywhere - even when they're traveling to remote locations. Also, the present invention is not restricted to securing only a particular (homogenous) environment. It operates across heterogenous platforms, which means that it can be used to control systems from any vendor or mix of vendors. This makes it far more applicable to an enterprise environment which can include any number of different vendors' platforms - both now and in the future.

[0014] These and other more specific aspects and advantages of the subject invention are demonstrated in particular in a distributed computing network that provides an adaptive capability to log a user located at one of a plurality of user workstations, onto one of a plurality of predetermined network servers, through the use of a single logon. In a preferred embodiment, a primarily local security server adapted to be connected to a user workstation, authenticates user identification information entered by a user at the workstation, or generates a failed logon signal in the event the user-provided authentication information is not valid for granting access to the local security server. A person server operating on the local security server then receives the failed logon signal from the local security server, identifies an alternate local security server ID in which the previously entered user name corresponds to a valid user, and transmits the alternate local security server ID back to the first local security server. When the first local security server receives the alternate local security server ID, it transmits the user identification information to the alternate local security server and the user is validated on the alternate local security server and logged onto the computer network.

[0015] It is another aspect of the present invention to achieve one or more of the above aspects and also provide a network access apparatus and method that allows a user to transparently communicate across a network comprised of a plurality of network communication protocols.

[0016] It is yet another aspect of the present invention to achieve one or more of the above aspects and also provide a network access apparatus and method that

first transmits a logon request from a user workstation to a local security server that either grants the authentication request or identifies a second local security server on the network that may grant the authentication request.

[0017] It is a further aspect of the present invention to achieve one or more of the above aspects and also provide a network access apparatus and method that evaluates a logon request by searching a local authentication database resident on a local security server to determine whether to grant a user access to the network via the local security server.

[0018] It is a still further aspect of the present invention to achieve one or more of the above aspects and also provide a network access apparatus and method that encrypts passwords stored in a local authentication database.

[0019] It is yet a further aspect of the present invention to achieve one or more of the above aspects and also provide a network access apparatus and method that accesses a network database resident in internal memory of a local security server to identify a second local security server on the network that may grant an authentication request, in the event the user is denied network access via the first local security server.

[0020] It is another aspect of the present invention to achieve one or more of the above aspects and also provide a network access apparatus and method that communicates authentication requests from a first local security server directly to a second local security server in the event the first local security server is unable to grant network access.

[0021] It is still another aspect of the present invention to achieve one or more of the above aspects and also provide a network access apparatus and method that automatically communicates authentication requests from a user workstation to at least one local security server without any user interaction.

[0022] It is another aspect of the present invention to achieve one or more of the above aspects and also provide a network access apparatus and method that maintains an audit log of all failed attempts to access network resources.

[0023] It is still another aspect of the present invention to achieve one or more of the above aspects and also provide a network access apparatus and method that monitors the number of failed attempts to access network resources and disables the network resource in the event the number of failed logon attempts exceeds a database number.

[0024] It is yet another aspect of the present invention to achieve one or more of the above aspects and also provide a network access apparatus and method that provides a redundant local security server capability wherein one or more standby servers can be used in the event a primary local security server is unavailable for any reason.

[0025] It is a further aspect of the present invention to achieve one or more of the above aspects and also provide a network access apparatus and method that allows a user to log onto the highest priority local security server available from any user workstation on the network, simply by entering a user name and password.

[0026] It is a further aspect of the present invention to achieve one or more of the above aspects and also provide a network access apparatus and method that maintains a single, centralized X.500 database of authorized network users on each local security server.

[0027] It is still a further aspect of the subject invention to achieve one or more of the above aspects and also provide a network access apparatus and method that maintains a map of connection information for each local security server operating on the enterprise.

[0028] It is yet a further aspect of the subject invention to achieve one or more of the above aspects and also provide a network access apparatus and method that utilizes a service mapping file server to periodically provide each associated workstation with an updated map of connection information for each local security server operating on the enterprise.

[0029] It is another aspect of the subject invention to achieve one or more of the above aspects and also provide a network access apparatus and method that maintains an updated map of connection information for each local security server by systematically polling the other local security servers on the enterprise.

[0030] It is still another aspect of the present invention to achieve one or more of the above aspects and also provide a network access apparatus and method that allows a user logged onto the network to access an assortment of network services based on the user's role.

[0031] It is yet another aspect of the present invention to provide a network access apparatus and method that maintains a single X.500 database on each local security server comprised of the users with their associated passwords that are authorized access to each local security server.

[0032] A preferred embodiment and more aspect, features and advantages of the present invention are explained in the following in more detail with respect to the drawings. It shows:

Fig. 1	a block schematic diagram of a typical wide area computer network;
Fig. 2	a block schematic diagram of a typical local computer network;
Fig. 3	a diagram of the structure of a local authentication database record;
Fig. 4	a diagram of the structure of a typical service mapping file record;
Fig. 5	a diagram of the structure of a typical network database record; and

Fig. 6a, 6b flowcharts depicting the computerized process of logging a user onto a network in accordance with the preferred embodiment of the present invention.

[0033] In the following detailed description of the preferred embodiment, reference is made to the accompanying drawings which form a part thereof, and in which is shown by way of illustration a specific embodiment in which the invention may be practiced.

[0034] This embodiment is described in sufficient detail to enable those skilled in the art to practice the invention and it is to be understood that other embodiments may be utilized and that structural changes may be made without departing from the scope of the present invention. The following detailed description is, therefore, not to be taken in a limited sense.

[0035] In this specification, the term "server" refers to a software process or set of processes that support some functionality. A local security server is a security access control software process to which end-users must authenticate before they can gain access to applications and systems on the computer network.

[0036] Referring to FIG. 1, in a computer network system or enterprise 10, computer workstations 11 and 21 are coupled to local security servers (LSSs) 12 and 22, respectively via communication links. 15 and 35, respectively. While FIG. 1 depicts a singular user workstation coupled to each LSS, it should be apparent to those of ordinary skill in the art that any number of workstations could be coupled to each LSS. Each local security server (12 and 22) is configured to allow multi-user access to the server only upon user authentication to the server. Once a user is granted access to the network via an LSS (12 and 22), the LSS acts as a gateway to provide the user access to all network services the server is otherwise authorized to access. An LSS can be designated as a default, primary, and/or standby LSS, depending upon the context. More specifically, a default LSS is an LSS designated in client software by a system administrator to act as a particular workstation's principal server such that when anyone attempts to access the network using the user workstation, the system will automatically route the request to the workstation's default LSS. A primary server, on the other hand, is an LSS that has been designated by a system administrator to function as the server that a particular user will always be logged onto whenever the user attempts to access the network. A standby server correspondingly, is an LSS with the same user information as a primary server. A standby server can be used when a user's primary server is unavailable for any reason. Each primary server can have one or more standby servers. It should be obvious to one of ordinary skill in the art that an LSS can serve multiple purposes for multiple workstations. Referring again to FIG. 1, LSS 12 can act as a default LSS for user workstation 11 and a standby server for user workstation 21, as well as a primary LSS for a particular user. In essence, one LSS can be the default LSS for some user workstations, the standby LSS for other workstations as well as the primary LSS for some users.

[0037] A client software process 40 (as shown in FIG. 2) operates on each computer workstation 11 and 21. When a user at a workstation wishes to gain access to the computer network, the client operating on the user workstation communicates the request for network access to a default LSS for authentication. The logical location and identity of a workstation's default LSS is a data value stored in the workstation's client. The default LSS may be the server located closest to the workstation or it may be another LSS operating elsewhere on the network. LSS 12 or LSS 22 in FIG. 1 could be the default server to workstation 11. LSS 22 or LSS 12 could also be the default server to workstation 21. It is important to note that the default LSS assigned to a workstation can be easily modified by a system administrator.

[0038] To add a new user to the network, a system administrator creates a new local authentication database record (FIG. 3) and copies the record into the internal memory of the LSS that is to become the new user's primary LSS. In the preferred embodiment, once a new record is copied into the primary LSS's local authentication database, the primary LSS will automatically route a copy of the new user record to all of the primary LSS's standby servers, as specified in the service mapping file (to be discussed later) which will result in the new user being automatically stored as a valid user in the standby server's memory. To enhance security, the entire record or at a minimum the user name and password can be encrypted prior to transmission to the standby server and then decrypted after receipt.

[0039] Also stored on each workstation is a service mapping file. As shown in FIG. 4, the service mapping file 41 contains a listing of all network LSSs with the name and logical location of their associated standby servers. The standby server is another LSS on the network with the same user information in its local authentication database as the default LSS. When a client attempts to access an LSS, if the LSS is not available its standby server will be invoked to process a logon request. A standby server is associated with a particular LSS through a network database entry. An example of one type of record which could be stored is described in FIG. 5. This network database entry may be entered into the system by a system administrator. Each record of the network database 43 is comprised of an LSS with its logical location and associated standby server names and logical locations together with the names of users authorized to log onto the LSS. In the preferred embodiment, the network database may be resident on disk storage of the LSS in the format of an X.500 or other suitable database.

[0040] Each LSS may be further coupled to the Internet or a similar computer network via communication links 20 and 40, respectively. As shown in FIG. 2, each LSS has access to a local authentication database 42

and a network database 43. These databases may be stored on either internal or external disk storage or any other suitable memory storage systems. A typical database record for the local authentication database 42 is depicted in FIG. 3. As shown in FIG. 3, each record at a minimum is comprised of a user name, password and user role. A user can have several local authentication database entries, each corresponding to a different role for the user. Examples of roles can include, but are not limited to "executive", "manager", "employee", etc. Roles can be related to, among other things, particular departments or positions within an organization. The user's role determines which network services can be accessed by the user. A network service may be an application program that has been properly installed on a server's internal disk memory. The services available and operable on each local security server are specified by a system administrator and installed on the server's disk storage when the local security is added to the network. Network services can be easily added, deleted or modified at any time by a system administrator. While this specification describes the invention with respect to a limited number of network services, it should be apparent to those of ordinary skill in the art that the number of network services is virtually unlimited. In the preferred embodiment, the local authentication database 42 is resident on disk storage of the LSS in the format of an X.500 or other suitable database. As is known by those of ordinary skill in the art, the X.500 database may also be resident in an external storage area.

[0041] As seen in FIG. 2, each LSS is comprised of a person server 31 and a service mapping file (SMF) server. The person server 31 is a software process operating on the LSS that receives all requests to log onto the network from a client 40, processes the requests and returns the results of a logon request back to the client 40. The person server 31 utilizes the user name/password combination received from the client to index into the local authentication database 42 stored in the server's disk storage. If the corresponding user name/password is stored in the local authentication database 42, the user will be connected to the local server. If the username/password combination is not found in the local authentication database, then the person server 31 searches the network database 43 (directory) to determine whether the user name exists on the enterprise. If the user name is found in the network database, the user authentication request is routed to the identified LSS for processing of the request. If, on the other hand, the user name is not found in the network database, the system will either deny the user's request or it may query the user to provide more information in order to process the authentication request.

[0042] The SMF server stores the service mapping file 41 on each LSS. As previously stated, the service mapping file 41 contains operational details of all servers on the enterprise. The SMF server 32 maintains an up-to-date "map" of the enterprise by periodically polling the network databases. All LSS's are defined in the network database under their server name and connection information (i.e., comms address). It is created from information in the network database 43 and it is updated regularly and passed down by the person server 31 to all workstations. While the preferred embodiment envisions a network wherein the person server 31 and the SMF server 32 are resident on the same platform, it also is possible for the person server and the SMF server to be resident on different platforms.

[0043] As seen in FIG. 1, multiple local computer networks may be coupled to the Internet to form a network of geographically separated and smaller computer networks consisting of a wide variety of computers and peripherals. The process of granting the user access to the computer network, as illustrated in FIG. 6, begins when a user at a workstation 11 attempts to log onto the computer network. The client 40 operating on the workstation presents a logon screen to the user (Step 600). In step 610, the user initiates the attempt to gain access by entering a user name and password into the local computer 11. The user name is a predetermined alphanumeric character string which uniquely identifies the user. It is typically assigned to the user by the system administrator who must ensure that the names are unique throughout the enterprise. The client 40 operating on the local computer captures the user's inputs and then in step 620, transmits the user-supplied information and the version number (FIG. 4) of the service mapping file 41 to the workstation's default LSS via communication link 15 or 35 (depending upon the particular workstation). The version number is essentially a time-stamp that indicates when the service mapping file was created. Each time a client 40 attempts to log onto an LSS, the LSS compares the client's service mapping file version number to the version number held by the SMF server 32. If the client's copy is out of date, the LSS returns the latest copy to the client 40. In this way, the client 40 always has the latest connection information for all LSSs on the network. In the event that a client's default LSS is not available, requiring the client 40 to access a standby LSS, the client would retrieve the connection information for a standby server on the network by accessing its copy of the service mapping file 41 stored in each workstation's disk storage (step 640). If a standby server is identified (step 650), the process returns to step 620 where the client 40 transmits the user information to the identified server. If a standby server is not identified, the client 40 displays a failed logon message (step 660) on the workstation's screen and the process terminates.

[0044] If it is determined in step 630 that the default server is available, the person server 31 operating on the LSS searches the local authentication database 42 (step 670) and attempts in step 680 to identify a single user name that corresponds to the entered user name and password. If a matching user name and password is found, the user is logged onto the network in step 690.

When a user is granted access to the network, the client software evaluates the user role associated with the previously provided user name and password combination to determine the complement of network services that the user will be entitled to access. For example, a user logged onto the network as a manager will be permitted to access those services available on the network that managers are authorized to utilize. If a user is logged onto a network as an employee, he/she will be permitted to access those services normally available to all employees. It is envisioned that the services available to a manager will likely be different than those available to all employees.

[0045] If a matching user name and password is not found, the person server 31 then searches the network database 43 (step 690) to determine whether the user name is recognized on the enterprise. In step 710, if no entry is found or if more than one matching entry is found, the person server 31 returns a failed logon message to the client 40 (step 720). Upon receipt of the message, the client 40 in step 730 displays the message on the workstation's display and the process terminates. While this specification describes the invention as if multiple matching entries from the network database 43 would lead to a failed logon response, it should be apparent to those of ordinary skill in the art that a number of other options could be employed without departing from the scope and intent of this invention. For example, the system could provide the user with an opportunity to manually input his/her LSS name or the system could give the user an opportunity to select a user name/LSS combination from a drop-down menu of retrieved user names. Once the user provides the proper LSS name or identifies the proper user name/LSS combination, the person server 31 returns the LSS name back to the client 40 and processing resumes in step 750. Even though this specification describes the invention wherein the person server transmits a local security ID back to a user workstation prior to the user workstation accessing the second local security, it should be apparent to those skilled in the art that the person server can establish a network connection, and therefore log a user onto the network, without returning logon functions to the user workstation.

[0046] If a single matching entry is found in step 740, the person server 31 in step 750 transmits the name of the user's primary LSS back to the client 40. Once the client receives the new LSS name, the process returns to step 620 where the client 40 retrieves the logical location of the new LSS from its service mapping file 41 and transmits the user information to the identified server. If no matching entries are found, the person server 31 (step 760) returns a failed logon message to the client 40. Upon receipt of the message, the client 40 (step 770) displays the message on the workstation's display and the process terminates. As a security precaution, the Person server 31 may log all failed attempts to access a local security server in an audit log to be periodically reviewed by the system administrator as a way of identifying security holes. The local security server may also monitor the number of failed attempts and may disable the terminal after a database number of failed attempts have been exceeded.

[0047] While this specification includes many details and specificities, these are only included for illustration and are not intended to limit the invention. Many modifications to the examples described above will be readily apparent to those of ordinary skill in the art which do not depart from the scope of the invention as defined by the following claims and their legal equivalents.

[0048] The method and apparatus to permit automated server determination for foreign system logon of the present invention may be used for automating authorized user access to a geographically dispersed network from any one of a plurality of user workstations. Moreover, the method and apparatus may be utilized where it is desirable to provide the capability for a user to log onto a network from any workstation on the network through the use of a single password. Furthermore, the method and apparatus to permit automated server determination for foreign system logon of the present invention may be used where it is desirable to provide the capability for a network to automatically identify a user's home server and to log the user onto the system in response to a user's entry of a single user name and password.

[0049] A method and apparatus is proposed for providing automatic user access authentication of any user who is a member of a set of authorized users of a computer enterprise from any one of a plurality of geographically dispersed user workstations, onto one of a plurality of predetermined local security servers, through the use of a single logon. A person server resident on a local security server compares the user-provided identification information to entries contained in a local authentication database. If the person server finds a match, the user is granted access to the local security server. If the person server does not find a match, the user-provided authentication information is not valid for granting access to the local security server and the person server then searches a network database to determine whether the entered user name is known to the enterprise. If the person server finds a single user name matching the previously entered user name, it returns the name of the local security server associated with the computer enterprise whose local authentication database may have the information necessary for allowing proper authentication of the user. Upon receiving the name of the newly-identified server, the client then automatically retrieves the server's logical location from a service mapping file and then repeats the authentication request to the new local security server. If the person server finds more than one user with the entered user name or if the person server fails to find any user name matching the previously entered user name, then it returns a failed logon request to the client. The system provides the capability

to operate across a number of network protocols through its use of a standard directory protocol, such as the X.500 standard.

Claims

1. Apparatus for automatic user access authentication by any user who is a member of a set of authorized users of a computer enterprise from any one of a plurality of geographically dispersed workstations operatively associated with the computer enterprise, comprising:

   client software operating with each of the associated workstations for interactively communicating with a prospective user who desires authentication for access to the computer enterprise to receive identification data from a prospective user seeking access at the associated workstation;

   a plurality of local security servers operatively connected to the workstations associated with the computer enterprise to receive and authenticate the identification information provided by each prospective user, each of said local security servers being associated with one or more, but not all, of the associated workstations and including:

   a local authentication database having the information necessary for allowing proper authentication of some, but not necessarily all, of the full set of authorized users of the computer enterprise;

   a network database directory having the information necessary for identifying a local security server associated with the computer enterprise whose local authentication database has the information necessary for allowing proper authentication of the full set of authorized users of the computer enterprise; and

   a person server for:

   allowing authentication for access of a prospective user when the identification data received from the client software at an associated workstation matches the data contained in the authentication database associated with said local security server; and

   communicating with the network database to identify a second local security server associated with the computer enterprise whose local authentication database may have the information necessary for allowing proper authentication of the user, and for causing the identification information to be supplied to the second local security server to allow authentication of the user without requiring further user activity when the user can not be authenticated through the local authentication database.

2. Apparatus according to claim 1, characterized in that each said local security server includes a service mapping file server for:

   maintaining an updated service mapping file, which preferably is comprised of a listing of local security servers with their associated connection information and a file version number; and

   providing said updated service mapping file to said plurality of user workstations associated with said local security server.

3. Apparatus according to claim 2, characterized in that said client software causes a version number of a service mapping file stored on said user workstation to be supplied to said local security server whenever said client attempts to log onto one of said plurality of local security servers, preferably wherein said service mapping file server compares said version number from said client software with said version number from said service mapping file stored on one of said plurality of local security servers and transmits an updated service mapping file to said user workstation in the event that a difference between the two version numbers exceeds a database value.

4. Apparatus according to any one of the preceding claims, characterized in that one of said plurality of local security servers causes said identification information to be supplied to said second local security server by transmitting the identification of said second local security server to said client software, preferably wherein said client software automatically transmits said authentication information to said second local security server to allow authentication of the user through said second local security server without requiring further user activity, more preferably wherein said client software accesses a service mapping file stored on said client workstation to identify the logical location of said second local security server.

5. Apparatus according to any one of the preceding claims, characterized in that one of said plurality of local security servers causes the authentication information to be supplied to said second local security server by transmitting the identification of said second local security server directly to said second local security server, and/or that the identification information is comprised of a user name, a user password and a user role, and/or that the local authentication database is comprised of a listing of users authorized to access one of said plurality of local security servers with their associated passwords and user roles, preferably wherein said client software:

maintains a database of user roles with at least one associated network service authorized for each user role; and

provides a logged-on user with access to said at least one network service that corresponds to said user's role.

6. Apparatus according to any one of the preceding claims, characterized in that said local authentication database is encrypted, preferably wherein said person server decrypts a user password contained in said local authentication database prior to authenticating a user for access, and/or that the network database is comprised of a listing of local security servers with their associated connection information, authorized users and standby local security servers, preferably wherein said standby local security server is a local security server whose local authentication database is identical to its associated local security server's local authentication database and/or preferably wherein said network database listing further includes the operational status of each said plurality of local security servers, in particular wherein said person server communicates with the network database to identify said associated standby local security server in the event that said local security server is not operational.

7. Apparatus according to any one of the preceding claims, characterized in that said plurality of local security servers create an audit entry for each unsuccessful user attempt to access said local security server, preferably wherein said audit entry is comprised of a workstation identity, with the date and time of the failed logon attempt and/or preferably wherein said plurality of local security servers disable a user workstation in the event the number of failed logon attempts exceeds a database value.

8. Apparatus for automatic user access authentication by any user who is a member of a set of authorized users of a computer enterprise from any one of a plurality of geographically dispersed workstations operatively associated with the computer enterprise, preferably according to any one of the preceding claims, wherein the apparatus comprises:

a plurality of local security servers operatively connected to the workstations associated with the computer enterprise to receive and authenticate the identification information provided by each prospective user, each of said local security servers being associated with one or more, but not all, of the associated workstations and including:

a network database directory having the information necessary for identifying a local security server associated with the computer enterprise that has the information necessary for allowing proper authentication of the full set of authorized users of the computer enterprise;

a person server for:

allowing authentication for access of a prospective user when the user's identification data matches the data contained in the authentication database associated with said local security server; and

communicating with the network database to identify a second local security server associated with the computer enterprise that may have the information necessary for allowing proper authentication of the user, and for causing the second local security server identification information to be returned to the user workstation, when the user can not be authenticated through a first local security server;

a service mapping file server for:

maintaining an updated service mapping file;
providing said updated service mapping file to said plurality of user workstations associated with said local security server; and

client software operating with each of the associated workstations for:

interactively communicating with a prospective user who desires authentication for access to the computer en-

terprise to receive identification data from said prospective user seeking access at the associated workstation;

interactively communicating with a first local security server to receive said updated service mapping file, and to authenticate said prospective user for access to said first local security server;

receiving a second local security server ID from said first local security server when the user can not be authenticated through said first local security server; and

routing said authentication information to said second local security server, utilizing said updated service mapping file, to authenticate the prospective user for access to said second local security server without requiring further user activity.

9. Apparatus according to any one of the preceding claims, characterized in that the service mapping file is comprised of a version number with a listing of local security servers and their associated logical locations, preferably wherein said client software causes a version number of a service mapping file stored on said user workstation to be supplied to said first local security server whenever said client software attempts to log onto said first security server, more preferably wherein said service mapping file server compares said version number from said client with said version number of said service mapping file stored on said first local security server and transmits an updated service mapping file to said client in the event that a difference between the two version numbers exceeds a database value.

10. Apparatus according to any one of the preceding claims, characterized in that each said plurality of local security servers are each further comprised of a local authentication database having the information necessary for allowing proper authentication of some, but not necessarily all, of the full set of authorized users of the computer enterprise, preferably wherein the identification information is comprised of a user name, a user password and a user role and/or preferably wherein said local authentication database is comprised of a listing of users authorized to access said local security server with their associated passwords and user roles, more preferably wherein said client software maintains a database of user roles with at least one associated network service authorized for each user role and provides a logged-on user with access to said network services that correspond to the user's role.

11. Apparatus according any one of the preceding claims, characterized in that the local authentication database is encrypted, preferably wherein said person server decrypts a user password contained in said local authentication database prior to authenticating a user for access, and/or that the network database is comprised of a listing of each local security server with their associated connection information, authorized users and standby local security servers, preferably wherein said standby local security server is a local security server whose local authentication database is identical to its associated local security server's local authentication database and/or preferably wherein said network database listing further includes the operational status for each local security server, in particular wherein said local security server communicates with the network database to identify an associated standby local security server in the event one of said plurality of local security servers is not operational.

12. Apparatus according to any one of the preceding claims, characterized in that said plurality of local security server creates an audit entry for each unsuccessful user attempt to access said person server, preferably wherein said audit entry is comprised of a workstation identity, with the date and time of the failed logon attempt and/or preferably wherein one of said plurality of local security servers disable a user workstation in the event the number of unsuccessful logon attempts exceed a database value.

13. Apparatus according to any one of the preceding claims, characterized in that the local authentication and network databases are X.500 or compatible databases.

14. Method for automatic user access authentication of any user who is a member of a set of authorized users of a computer enterprise from any one of a plurality of geographically dispersed workstations operatively associated with the computer enterprise, the computer enterprise includes a plurality of local security servers each coupled to client software operating on a user workstation, wherein each of said local security servers is associated with one or more, but not all, of the workstations associated with the computer enterprise, each local security server is comprised of a person server, a local authentication database, a service mapping file server and a network database, wherein the method comprises the computer-implemented steps of:

receiving identification data at a client and forwarding the authentication data from the client

software to a first local security server;

at the first local security server, allowing authentication for access of a prospective user when the identification data received from the client software matches the data contained in the authentication database associated with the first local security server; and

communicating with the network database to identify a second local security server associated with the computer enterprise whose local authentication database may have the information necessary for allowing proper authentication of the user, and for causing the identification information to be supplied to the second local security server to allow authentication of the user, without requiring further user activity, when the user can not be authenticated through the local authentication database associated with the first local security server.

15. Method according to claim 14, characterized in that the service mapping file server performs the following computer-implemented steps:

maintaining an updated service mapping file; and
providing said updated service mapping file to the plurality of user workstations associated with the local security server.

16. Method according to claim 15, characterized in that the service mapping file is comprised of a version number with a listing of local security servers and their associated logical locations, preferably wherein the client software performs the step of causing a version number of a service mapping file stored on said user workstation to be supplied to said first local security server whenever said client attempts to log onto said first local security server, more preferably wherein the service mapping file server performs the computer-implemented step of comparing the version number from the client with the version number of the service mapping file stored on the first local security server and transmitting an updated service mapping file to the client in the event that a difference between the two version numbers exceeds a database value.

17. Method according to claim 15 or 16, characterized in that said step of causing the identification information to be supplied to the second local security server, comprises the computer-implemented step of transmitting the identification of the second local security server from the first local security server to the client workstation, preferably wherien the client software performs the computer-implemented steps of receiving a local security server ID from the first local security server and routing the authentication information to the second local security server to authenticate the prospective user for access to the second local security server without requiring further user activity, more preferably wherein said step of routing the authentication information to the second local security server comprises the step of accessing the service mapping file to identify the logical location of the second local security server.

18. Method according to any one of claims 14 to 17, characterized in that said step of causing the identification information to be supplied to a second local security server, comprises the computer-implemented step of transmitting the authentication information directly to the second local security server from the first local security server, and/or that the identification information is comprised of a user name, a user password and a user role, and/or that each local authentication database is comprised of a listing of users authorized to access each said plurality of local security servers with their associated passwords and user roles, preferably wherein said client software performs the following computer-generated steps:

maintaining a listing of user roles with at least one network service authorized for each role; and

providing a logged-on user with access to said network services that correspond to the user's role.

19. Method according to any one of claims 14 to 18, characterized in that the local authentication database is encrypted, preferably wherein the person server decrypts a user password contained in the local authentication database prior to authenticating a user for access, and/or that the network database is comprised of a listing of local security servers with their associated connection information, authorized users and standby local security servers, preferably wherein the standby local security server is a local security server whose local authentication database is identical to its associated local security server's local authentication database and/or preferably wherein the network database listing further includes the operational status for each local security server, in particular wherein the step of communicating with the network database to identify a second local security server associated with the computer enterprise further comprises the computer-implemented step of identifying an associated standby local security server in the event the local security server is not operational.

20. Method according to any one of claims 14 to 19, characterized in that the person server performs the step of creating an audit entry for each failed attempt to access said person server, and/or that the audit entry is comprised of a workstation identity, with the date and time of the failed logon attempt, preferably wherein the person server additionally performs the step of disabling a user workstation in the event the number of failed logon attempts exceeds a database value, and/or that the local authentication and network databases are X.500 or compatible database.

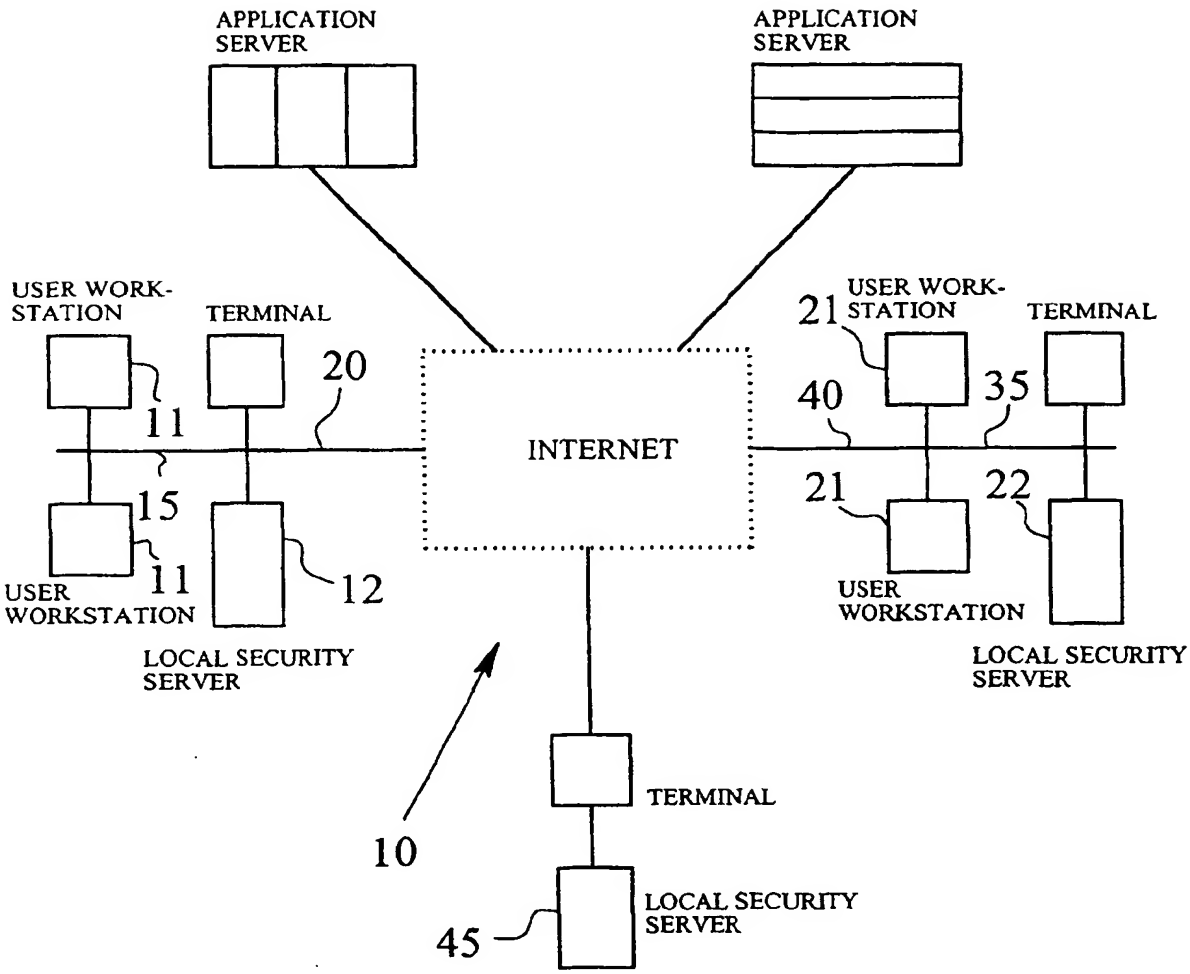

Fig. 1

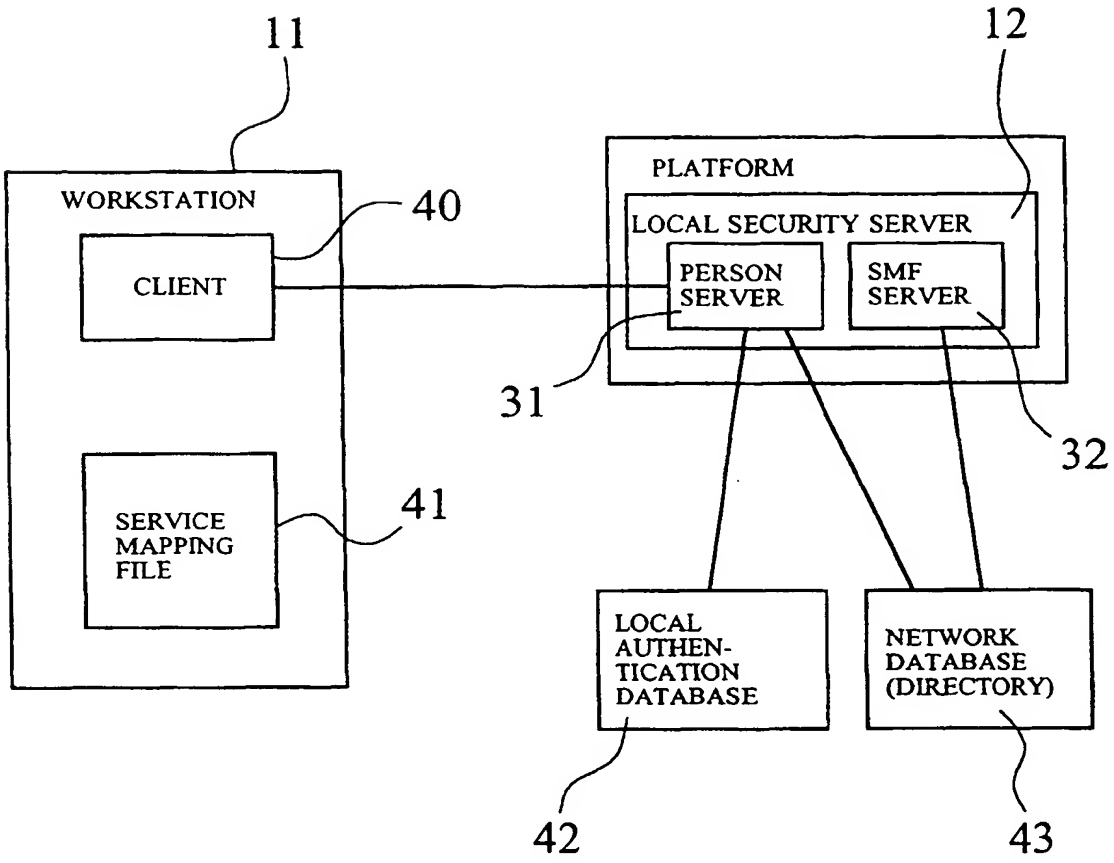

Fig. 2

USERNAME	Alphanumeric ‹ 10 characters
PASSWORD	Alphanumeric ‹ 10 characters
USER ROLE	Alphanumeric ‹ 10 characters

Local Authentication Database Record

FIG. 3

Local Security Server Name	Alphanumeric
#1 Standby Server Name	Alphanumeric
#1 Stadby Server Logical Location	Alphanumeric
#2 Standby Server Name	Alphanumeric
#2 Standby Server Logical Location	Alphanumeric
Service Mapping File Version Number	Numeric

Service Mapping File Record

FIG. 4

Local Security Server Name	Alphanumeric
LSS Logical Location	Alphanumeric
#1 Standby Server Name	Alphanumeric
#1 Standby Server Logical Location	Alphanumeric
#2 Standby Server Name	Alphanumeric
#2 Standby Server Logical Location	Alphanumeric
Authorized User #1	Alphanumeric
User #1 Password	Alphanumeric
Authorized User #2	Alphanumeric
User #2 Password	Alphanumeric

Network Database Entry Record

FIG. 5

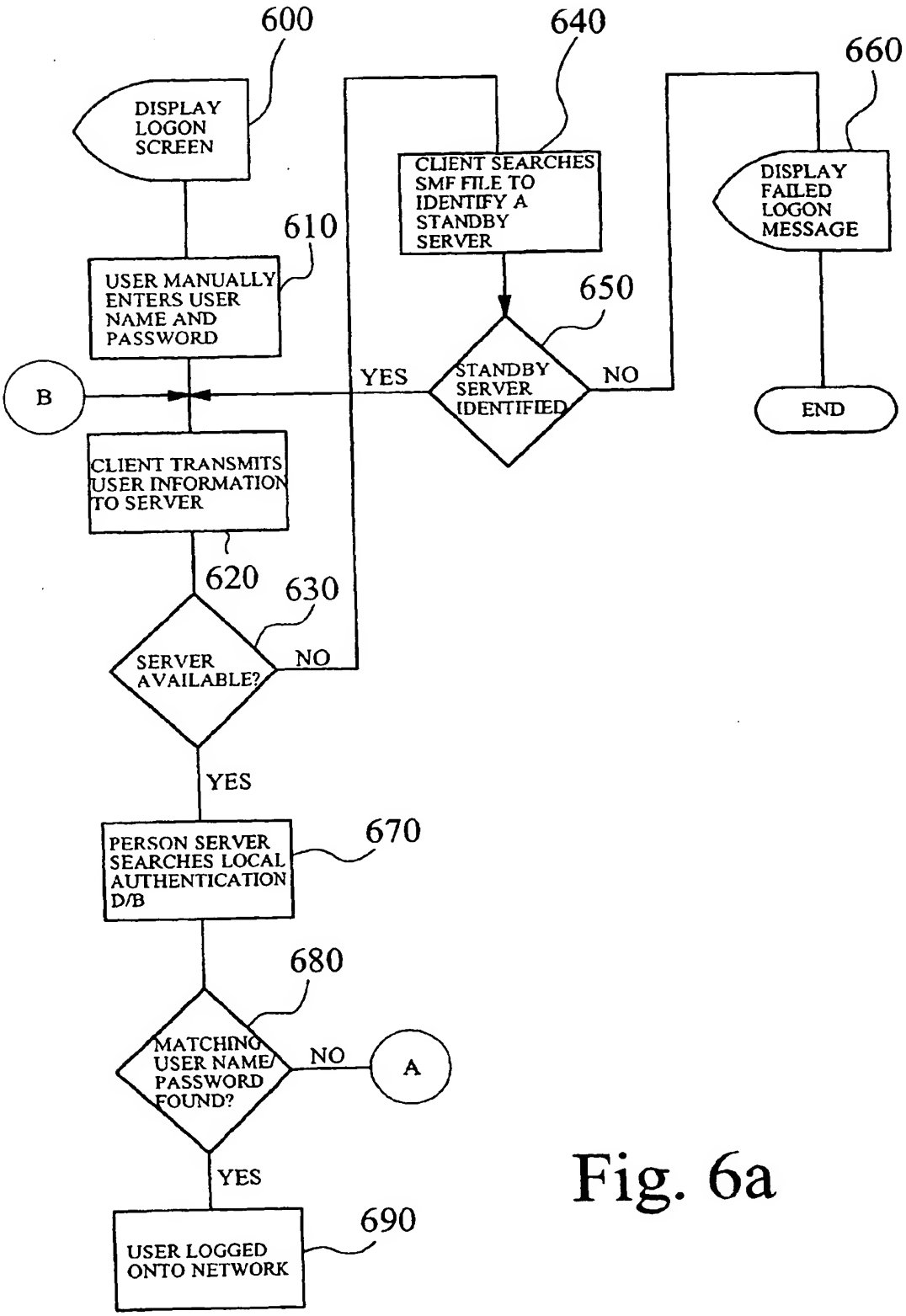

Fig. 6a

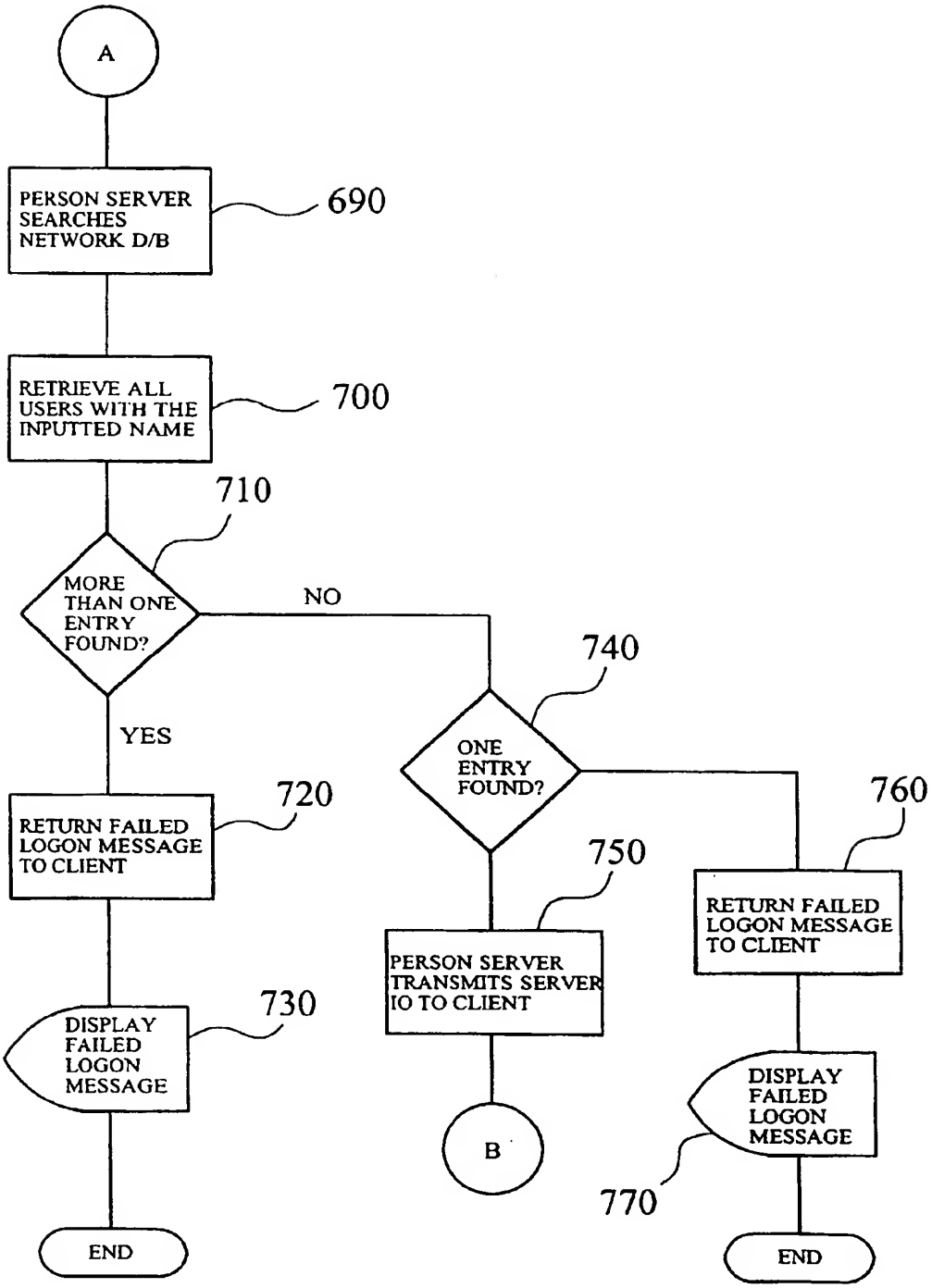

Fig. 6b

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 12 5760

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	EP 0 570 683 A (IBM) 24 November 1993 (1993-11-24) * abstract * * column 2, line 24 - column 3, line 33 *	1,2,5,8, 14,16,18	G06F1/00 H04L29/06
A	"PARTIAL CONTAINMENT STRUCTURE FOR INEGRATION OF DISTRIBUTED COMPUTING ENVIRONMENT AND LOCAL REGISTRIES" IBM TECHNICAL DISCLOSURE BULLETIN,US,IBM CORP. NEW YORK, vol. 38, no. 9, 1 September 1995 (1995-09-01), pages 535-538, XP000540357 ISSN: 0018-8689 * the whole document *	1,8,14	
A	US 5 586 260 A (HU WEI-MING) 17 December 1996 (1996-12-17) * abstract; figures 3,4 * * column 3, line 46 - column 5, line 58 * * column 7, line 6 - line 10 *	1,2,5,8, 14,16,18	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

G06F
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	6 April 2000	Sigolo, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 12 5760

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

06-04-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0570683 A	24-11-1993	US 5642515 A	24-06-1997
		JP 2022773 C	26-02-1996
		JP 6029993 A	04-02-1994
		JP 7054935 B	07-06-1995
US 5586260 A	17-12-1996	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82